U.S. Department of Justice

Criminal Division

Child Exploitation and Obscenity Section

1400 New York Ave., NW
Suite 600
Washington, DC 20530
(202) 514-5780 FAX: (202) 514-1793

November 7, 2014

Joseph F. Gross, Esq.

Re: United States v. Kirk Cottom; 13CR108

Dear Counsel:

Pursuant to Rule 16(a)(1)(G) of the Federal Rules of Criminal Procedure, the government hereby discloses that it intends to elicit testimony from Paul Ferraro and Adrian Cartegena under Federal Rules of Evidence 702, 703, or 705. Pursuant to Rule 16(b)(1)(C) of the Federal Rules of Criminal Procedure, the government hereby requests from defendant disclosure of testimony he intends to use under Rule 702, 703 and/or 705 of the Federal Rules of Evidence as evidence at trial.

Mr. Ferraro and Mr. Cartegena are Information Technology Specialist Forensic Examiners with the Federal Bureau of Investigation. Their CV's are attached. You were previously provided with copies of their forensic reports, dated August 30, 2013 and November 21, 2013. Please note that the evidence they examined, including all "derivative evidence" referred to in the referenced forensic reports, have been and remains available for your inspection and review. Mr. Ferraro and Mr. Cartegena may testify regarding all matters referenced in their forensic reports, including those contained on the referenced derivative evidence. In particular, Mr. Ferraro and Mr. Cartegena may testify regarding their examination of your client's electronic devices, which are specified in the forensic reports. Their testimony will be based upon their knowledge, skills, training and experience in the area of computer forensics, computer forensic data acquisition and analysis, investigations in child exploitation cases, the Internet, and their forensic analysis of your client's digital media. As part of their testimony, they may also testify regarding the Internet, the forensic examination of computers and digital media, and how the Internet is used to trade child pornography. Specifically, they may testify:

- regarding the Internet, which is a collection of computers and computer networks which are connected to one another via high-speed data links and telephone lines for the purpose of communicating and sharing data and information;

- that connections between Internet computers exist across state and international borders; and that the Internet is a means of interstate and international communication; indeed, information sent between two computers connected to the Internet frequently crosses state and international borders even when the two computers are located in the same state;

- regarding modems, and how a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world;

- regarding Internet Service Providers. Individuals and businesses obtain access to the Internet through businesses known as Internet Service Providers ("ISPs"). ISPs provide their customers with access to the Internet using telephone or other telecommunications lines; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers; remotely store electronic files on their customers' behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or businesses that have subscriber accounts with them. Those records often include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, and other information both in computer data and written record format;

- regarding IP Addresses. An Internet Protocol address ("IP address") is a unique numeric address used by each computer on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be properly directed from its source to its destination. Most ISPs control a range of IP addresses;

- that when a customer logs into the Internet using the service of an ISP, the computer used by the customer is assigned an IP address by the ISP. The customer's computer retains that IP address for the duration of that session (i.e., until the user disconnects), and the IP address cannot be assigned to another user during that period;

- regarding four basic functions computers and the Internet serve in connection with child pornography: production, communication, distribution, and storage;

- regarding how individuals can use computers and the Internet to meet, communicate with each other, and share files, including but not limited to websites, chat rooms, message boards, email, instant messaging, news groups, social networking sites, peer-to-peer programs, ICQ;

- regarding how child pornographers can transfer non-digital photographs from a camera into a computer-readable format a scanner, and how digital cameras allow images to be transferred directly onto a computer. Digital cameras often embed information into digital pictures, known as metadata, that identifies the camera used to take the picture;

- regarding how a computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media

(commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store hundreds of thousands of images and videos at very high resolution;

- regarding how digital images/videos can be stored on external storage media such as thumb drives, compact disks, external hard drives, mp-3 players, smart phones, and how digital images/videos can be easily transferred from one digital device to another;

- regarding dedicated online storage space, such as the "FTP," or "File Transfer Protocol" site, and how such a site allows Internet users to maintain a massive and secure private library of child pornography that is available for viewing or download only by a certain group of individuals, such as members of the PedoBook online bulletin board;

- regarding user-created message boards, and how they can be easily created with free or inexpensive software and commercial web hosting companies;

- regarding forensic hashing, which is the process of using a mathematical function, often called an algorithm, to generate a numerical identifier for data (such as a particular file). If the data is changed, even very slightly (such as the addition or deletion of a comma or a period), the identifier should change. A hash value can be thought of as a "digital fingerprint" for data;

- regarding the use of a "hash set" which contains the hash values of image and video files associated with known identified victims of child pornography to determine whether these files are stored within a digital device;

- The process of obtaining and verifying an image of a computer media item, bit-stream copies, and Message-Digest algorithm 5 (MD5) hash values;

- Specialized computer terms, including, but not limited to, terms mentioned in this notice and in his report, such as ".html," ".lnk" ".jpg," ".mpg," ".avi," "cookie file," and "file slack;"

- Evidence of web browsing activity and e-mail communications, including, but not limited to, fragments of web pages accessed, cookie files, e-mail messages, and other Internet-based communications stored in locations including, but not limited to, the temporary Internet file folders, file slack, and unallocated space.

Please contact me, Trial Attorney Keith Becker or Assistant U.S. Attorney Michael Norris if you have any questions about any of the information provided.

Sincerely,

/s/ Sarah Chang
Sarah Chang
Trial Attorney
Child Exploitation and Obscenity Section
Criminal Division
United States Department of Justice

Enclosures